UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/920,057	08/01/2001	Valtteri Niemi	324-010477-US (PAR)	4430

2512 7590 12/05/2008

PERMAN & GREEN
425 POST ROAD
FAIRFIELD, CT 06824

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
12/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/920,057	NIEMI ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32 and 47-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-8,11,12,17,19-21,23-30,49 and 50* is/are rejected.

7)☒ Claim(s) *3,9,10,13-16,18,22,31,32,47,48,51 and 52* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A response was received on 16 September 2008. By this response, Claims 1-3, 6, 15, 17-19, 22, 31, 47, and 48 have been amended. Claims 33-46 have been canceled. New Claims 49-52 have been added. Claims 1-32 and 47-52 are currently pending in the present application.

Response to Amendment

2. A supplemental reply was received on 18 September 2008. As per 37 CFR 1.111(a)(2)(i), a supplemental reply is generally not entered as a matter of right. Because the supplemental reply proposes the addition of new claims 53 and 54, it is not clearly limited to the responses provided for by 37 CFR 1.111(a)(2)(i). Further, the supplemental reply does not fully comply with the requirements of 37 CFR 1.121(c), because at least Claims 51 and 52 are not listed with the correct status identifiers. Although the claims are listed as (Previously Presented), the claims include markings showing amendments, and therefore should have been listed as (Currently amended). Therefore, the supplemental reply will not be entered because it is not limited to the responses provided for by 37 CFR 1.111(a)(2)(i) and because it is not fully compliant with 37 CFR 1.121.

Response to Arguments

3. Applicant's arguments filed 16 September 2008 have been fully considered but they are not persuasive.

Regarding the previous rejection of Claims 1-8, 11, 12, 17-24, 27, 28, 33-40, 43, and 44 under 35 U.S.C. 103(a) as unpatentable over the 3rd Generation Partnership Project technical specifications (collectively referred to as "3G"), Applicant argues that it would not have been obvious to use the same encryption algorithm in a wideband CDMA network and a packet-switched TDMA network as claimed.

In particular, Applicant asserts that the "claimed subject matter did not start from a handover scenario" and that "the starting point of the claimed subject matter was different" (page 13 of the present response). However, the Examiner notes that the present invention did appear to be based at least partly on requirements imposed by handover scenarios (see page 2, lines 17-18, of the present specification, where one of the requirements is synchronization, for example, in connection with handover; see also page 3, lines 14-15, of the present specification, where user equipment is capable of contacting both types of network, and therefore handover must have been considered). Applicant further asserts that, faced with the requirement of an encryption algorithm for GPRS, the "most natural choice would have been to design a suitable encryption algorithm" (page 13 of the present response, implicitly in contrast with the use of a pre-existing algorithm). However, this explicitly contradicts Applicant's statement in the

present disclosure that "[d]esigning a new encryption algorithm is a very demanding operation" (page 3, lines 10-11 of the present specification).

Applicant further alleges that the "statement that it would have been obvious to try using the same algorithm or two different algorithms in the two systems is conclusory and speculative" and that the statement "does not reflect the way the skilled person would have encountered and addressed the problem of designing an encryption algorithm" (page 13 of the present response). However, the Examiner submits that one of ordinary skill in the art would have recognized that design of an encryption algorithm would have been a significant undertaking (as recognized by Applicant's specification, noted above) and that prior to attempting such a design, one of ordinary skill in the art would have looked to known encryption algorithms to determine whether a known algorithm would meet the requirements that needed to be satisfied for the new application, due to simple expedience. Although Applicant asserts that "there were, theoretically, an infinite number of choices" for the algorithm and that there "were no limitations for the algorithm" (page 13 of the present response), this is contradicted by the present disclosure, noting that specific requirements (i.e. limitations) for the algorithm were set forth (see page 2, lines 14-24 of the present specification). Further, although Applicant asserts that there were an infinite number of choices, the Examiner notes that there were clearly a finite number of encryption algorithms available at the time of the filing of the present application, and further notes that the choice as particularly framed in the previous Office action was simply the dichotomy between using either the same algorithm in the two networks types or two different algorithms,

one in each network type. This choice between two options is clearly a finite number of choices to be considered and/or tried.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning (pages 13-14 of the present response), it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). Further, in response to applicant's argument that one attempting to address "the problem solved by Applicant using the required criteria" would not have taken into account considerations of processing overhead but would only have used Applicant's requirement (pages 13-14 of the present response), the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985). Specifically, although Applicant alleges that a reduction in overhead is speculative (pages 13-14 of the present response), the Examiner submits that it would have been clear to one of ordinary skill in the art that using the same encryption algorithm in the two network types would have reduced processing overhead, because if different algorithms were used, then all data would have had to be decrypted from the first algorithm and re-encrypted under the second algorithm

whenever handover occurred, therefore requiring significantly greater processing power and time, i.e. overhead. Further, although Applicant argues that one of ordinary skill would not have used overhead considerations as a motivation to combine or modify references, the Examiner submits that one of ordinary skill in the art would certainly have considered the processing power and time requirements (i.e. overhead) when considering the options. These considerations are taken into account in virtually all computer and communications situations, where lower processing power and processing time are virtually always desirable. In particular, especially at the time of filing of the present application, mobile devices had significantly lower processing and memory capabilities than normal computers, and therefore it would be highly desirable to reduce the processing overhead required, especially with respect to such a processor intensive application as encryption.

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Claim Objections

4. Claims 3, 47, 48, 51, and 52 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim cannot depend from any other multiple dependent claim. Further, Claims 18, 22, 31, 32, 51, and 52 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim

should refer to other claims in the alternative only. See MPEP § 608.01(n). Accordingly, the claims have not been further treated on the merits.

5. Claim 1 is objected to because of the following informalities:

Claim 1 recites "A method in a mobile system in a mobile system" in the preamble. It appears that one instance of "in a mobile system" should be deleted.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 2, 17, 19-21, 23-30, and 50 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 2 recites the limitation "the agreed format". Although there is reference to a format in Claim 1, there is no reference to an "agreed format"; however, for purposes of interpreting the prior art, "the agreed format" has been assumed to refer to the format recited in Claim 1.

Claim 17 recites the limitation "means for encrypting data to be transmitted of a packet-switched time division multiple access mobile system" in lines 3-4 of the claim. It is not clear what the phrase "of a packet-switched [TDMA] mobile system" is intended to

modify. Further, the claim recites "the user equipment" in line 11 of the claim. There is insufficient antecedent basis for this limitation.

Claims 20, 21, and 23-30 are directed to "User equipment", however, Claim 17, from which they depend, is directed to an apparatus.

Claim 50 recites the limitation "means for decrypting data received using an encryption algorithm" in line 2. It is unclear how the encryption algorithm is used to receive the data (noting that the placement of the phrase "using an encryption algorithm" indicates that it modifies "received"). Further, the phrase "a radio access network of a packet switched time division multiple access mobile system employing a wideband code division multiple access method of a universal mobile telecommunications system" in lines 4-7 is generally unclear. First, it is not clear whether the network uses TDMA or WCDMA since both are recited. Further, the use of the general protocol name "universal mobile telecommunications system" renders the claim scope uncertain because protocols are subject to evolving standards and go through several version revisions, and therefore the protocol name cannot be used to properly identify the specific methods, standards, or products that are associated with the protocol name.

Claims not explicitly referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 2, 4-8, 11, 12, 17, 19-21, 23, 24, 27, 28, 49, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over the 3rd Generation Partnership Project technical specifications, specifically 3G TS 33.102, version 3.2.0, published October 1999; 3G TS 25.301, version 3.4.0, published March 2000; 3G TS 25.401, version 3.1.0, published January 2000; and 3G TS 25.832, version 3.0.0, published October 1999 (hereinafter collectively referred to as "3G").

In reference to Claim 1, 3G discloses a method for transmitting data in a mobile system that includes encrypting data to be transmitted between a network using packet-switched TDMA and a user mobile equipment (see 3G TS 33.102, page 48, section 8.2.2; 3G TS 25.301, pages 39-41, chapter 8), and that handover can occur between a wideband CDMA network and a packet-switched TDMA network (see 3G TS 25.401, pages 17-18, section 7.2.3, where handover may occur between UMTS and GSM systems, where UMTS uses wideband CDMA and GSM uses packet-switched TDMA; also 3G TS 33.102, pages 33-34, section 6.6.4, where cipher keys are transmitted between the MSC/VLRs during handover and/or new keys can be generated or converted as necessary, and pages 37-41, section 6.8, describing conversion functions

between authentication in UMTS and GSM; see also 3G TS 25.832, pages 6-12, chapter 5, especially sections 5.6 and 5.7). While these specifications do not explicitly specify that the same encryption algorithm is used in the two types of networks, the above sections do disclose adapting parameters between the wideband CDMA and packet-switched TDMA networks (again, see 3G TS 33.102, pages 33-34 and 37-41, as cited above). Further, it would have been obvious to one of ordinary skill in the art to use the same encryption algorithm in the two network types between which handover takes place; given the finite number of choices of algorithms, and more particular, the choice between using the same algorithm or two different algorithms in the two systems, it would have been obvious to try the two different options. It would have further been rendered obvious to use the same encryption algorithm between networks between which handover takes place, in order to realize the predictable result of reducing overhead as compared to using two different algorithms (where if two different algorithms were used, then all data would have to be decrypted from the first algorithm and re-encrypted under the second algorithm whenever handover occurred).

Similarly, in reference to Claim 49, 3G discloses a method for transmitting data in a mobile system that includes decrypting received data that was transmitted between a network using packet-switched TDMA and a user mobile equipment (see 3G TS 33.102, page 48, section 8.2.2; 3G TS 25.301, pages 39-41, chapter 8), and that handover can occur between a wideband CDMA network and a packet-switched TDMA network (see 3G TS 25.401, pages 17-18, section 7.2.3, where handover may occur between UMTS and GSM systems, where UMTS uses wideband CDMA and GSM uses packet-

switched TDMA; also 3G TS 33.102, pages 33-34, section 6.6.4, where cipher keys are transmitted between the MSC/VLRs during handover and/or new keys can be generated or converted as necessary, and pages 37-41, section 6.8, describing conversion functions between authentication in UMTS and GSM; see also 3G TS 25.832, pages 6-12, chapter 5, especially sections 5.6 and 5.7). While these specifications do not explicitly specify that the same encryption algorithm is used in the two types of networks, the above sections do disclose adapting parameters, i.e. creating input parameters of a required format, between the wideband CDMA and packet-switched TDMA networks (again, see 3G TS 33.102, pages 33-34 and 37-41, as cited above). Further, it would have been obvious to one of ordinary skill in the art to use the same encryption algorithm in the two network types between which handover takes place; given the finite number of choices of algorithms, and more particular, the choice between using the same algorithm or two different algorithms in the two systems, it would have been obvious to try the two different options. It would have further been rendered obvious to use the same encryption algorithm between networks between which handover takes place, in order to realize the predictable result of reducing overhead as compared to using two different algorithms (where if two different algorithms were used, then all data would have to be decrypted from the first algorithm and re-encrypted under the second algorithm whenever handover occurred).

In reference to Claim 2, 3G further discloses that a format of the parameters includes a number and length of each parameter (3G TS 25.301, pages 40-41).

In reference to Claims 4 and 5, 3G further discloses a counter parameter (3G TS 25.301, pages 40-41, section 8.2.2.1).

In reference to Claim 6, 3G further discloses the use of a bearer parameter (3G TS 25.301, page 41, section 8.2.2.3).

In reference to Claims 7, 8, 11, and 12, 3G further discloses that the encryption algorithm can be executed in either the MAC layer or the RLC layer and that the counter parameter includes a frame number (3G TS 25.301, pages 40-41, section 8.2.2.1).

Claims 17, 20-24, 27, 28, and 50 are directed to an apparatus that corresponds substantially to the methods of Claims 1, 4-8, 11, 12, and 49, and are rejected by a similar rationale.

In reference to Claim 19, it would have further been obvious to one of ordinary skill in the art at the time the invention was made for the implementation of the encryption algorithm to be the same in both the packet-switched TDMA network and the wideband CDMA network, for the reasons detailed above, namely that it would have been obvious to try the finite options available, and it further would have been obvious in order to realize the predictable result of reducing overhead as compared to using algorithms that are implemented differently.

Allowable Subject Matter

10. Claims 9, 10, and 13-16 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

11. Claims 25, 26, 29, and 30 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

12. Reasons for indicating allowable subject matter were set forth in the Office action mailed 04 April 2006.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ZAD/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437